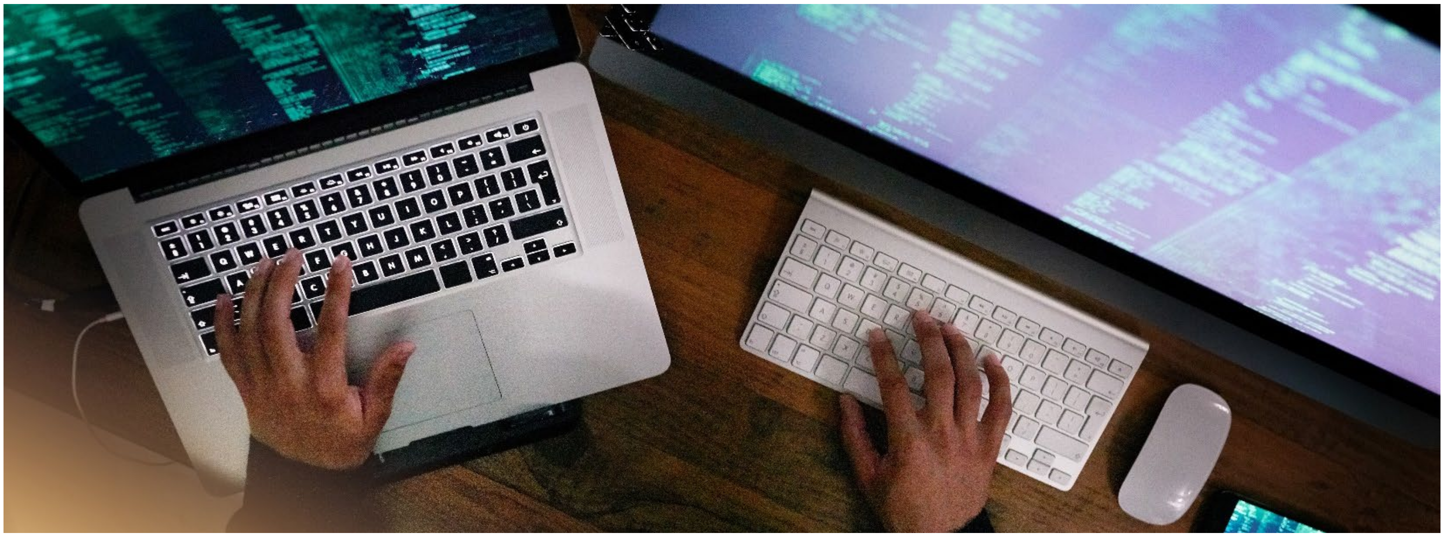
UNISON
RISK ADVISORS



UnisonRiskAdvisors.com | March 15, 2022

Cyber Risk Advisory: The Russia/Ukraine Conflict

As the world watches the Russian invasion of Ukraine unfold, a close eye should be kept on a different kind of battlefield as well; cyberspace. While we have long known the capabilities of Russian cybercriminal groups, the lines between state-sponsored and independent criminal actors are beginning to blur. For example, shortly after Russia's invasion and amidst a flurry of sanctions laid down by the United States and other NATO countries, notable ransomware gang Conti publicly announced its support of the Russian government.

While there is no measurable increase in ransomware activity in the United States just yet, that could change. Conti and other cyber gangs from Russia currently have Ukraine in their crosshairs, but cyber vigilance should be practiced around the globe.

The Threats and Cyber Protocols

As more organizations cease conducting business with Russia, it's easy to imagine cybercriminals shifting gears once the dust begins to settle. While industries such as healthcare and banking are heavily regulated when it comes to cybercrime, industries like infrastructure and manufacturing are not.

It will be important to look out for fraudulent activities such as phishing, wire transfer fraud, and fraudulent fundraising efforts in the coming months. Cybercriminals thrive when they can play on the emotions of their victim, as evidenced by the spike in cybercriminal activity during the onset of the COVID-19 pandemic.

In response to these growing threats, businesses should emphasize the basics of cyber security and listen to their IT teams' guidance. Training employees on proper cyber hygiene practices, such as regular password changes and implementing multi-factor authentication (MFA) protocols, is strongly recommended for building a solidified first line of defense.

Blocking IP addresses from Russia and Ukraine as well as .ru websites is also strongly recommended. However, while these protocols may ease concerns, keeping a watchful eye on who is allowed into your network is more critical than ever. Adding Indicators of Compromises (IoCs) to systems for things like HermeticWipers, Distributed Denial of Service (DDoS) attacks, and Russia-Ukraine domains is a good way to closely monitor activity.

Cyber Insurance: More Critical Than Ever

Ensuring that the members of an organization follow fundamental preventative cyber hygiene protocols is not only crucial for preventing a cyberattack from happening in the first place, it is also critical for obtaining an adequate cyber liability insurance policy.

Cyber premiums are at all-time highs, and as the market continues to harden, underwriters are more stringent than ever. Many underwriters require businesses to have a certain protocol level before even writing a cyber policy.

When obtaining a cyber insurance policy, businesses should ensure that the policy includes a cyber terrorism carveback. These carvebacks, however, have largely been untested thus far.

Disaster Recovery

As we have seen from notable cyberattacks like the Colonial Pipeline data breach, disruptions for supply chains and energy grids can easily create a public panic. While we have talked about preventative measures at length, the current climate also creates a need for disaster plans following a devastating attack.

A full-fledged contingency plan should also be in place in the event of service or operational interruptions due to a cyberattack. Businesses should ensure that equipment such as generators and backup servers are functional and ready to run if needed.

Resources

There are several essential resources to consider for the potential virtual battlefield. The FBI's Internet Crime Complaint Center (IC3) is a one-stop shop to see what's happening in the world of cybercrime and will be the first to report all instances of cyberattacks. Victims of cyber incidents should report crimes to IC3 immediately to help raise awareness.

Another resource is the Cybersecurity & Infrastructure Security Agency (CISA). CISA's website is full of free resources for businesses to implement, including a cyber hygiene program.

Additionally, MRK Technologies has created a 20-point "preparing for cyberwar" checklist. This checklist can help businesses assess their readiness for potential cyberwarfare.

Conclusion

The conflict between Russia and Ukraine is extremely unsettling and calls for a return to the basics from a cyber perspective. Regular training, ensuring awareness and creating a culture of caution will be fundamental for what's on the horizon.

(*Sources:* *cpomagazine.com*, *bloomberg.com*, *ic3.gov*, *cisa.gov*, *mrktech.com*)

Note: This communication is for informational purposes only. *Although every reasonable effort is made to present current and accurate information, Unison Risk Advisors makes no guarantees of any kind and cannot be held liable for any outdated or incorrect information.*